Jericho Forum Introduction

www.jerichoforum.org

Stephen T. Whitlock

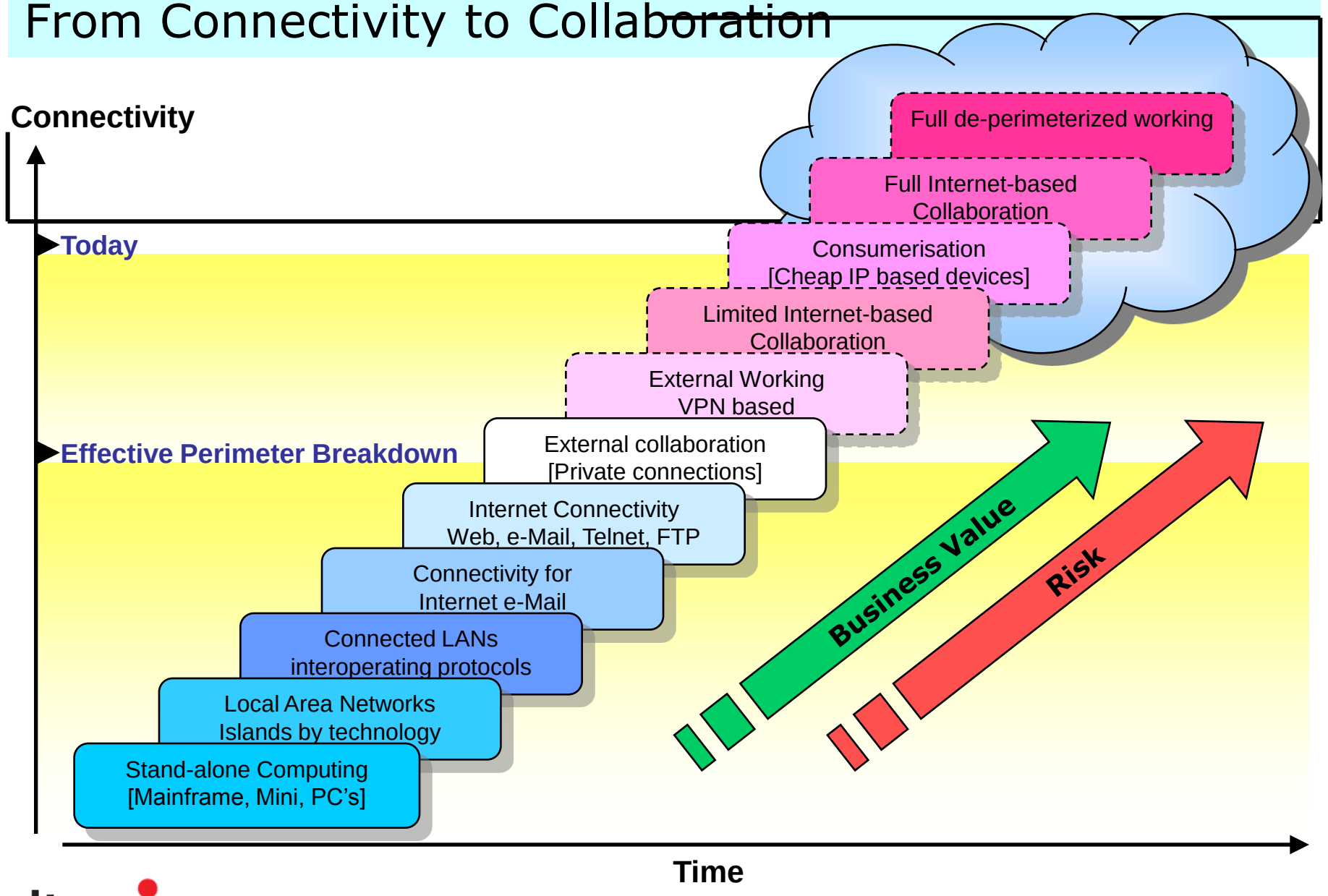
Representing the

Board of Management of the Jericho Forum

Brief History

- In 2004, Jericho Forum thought leaders asked the IT industry the question:
  - *When corporate perimeters crumble due to business drivers demands for greater connectivity with collaborators over the Internet:*
    - How do you secure it?
    - How do you collaborate in it?"
- We called the crumbling perimeters problem ***deperimeterization***
- We analyzed the architectural space that needs to be secured
- We wrote "position papers" on many of these, and have delivered two key deliverables:
  - Design Principles (Jericho Forum Commandments)
    - Questions that evaluate how far IT architecture meets the criteria for secure operation in a deperimeterized environment
    - The implications are that that your IT systems should work the same way irrespective of whether you are inside or outside your corporate perimeter
  - Collaboration Oriented Architectures (COA) Framework
    - Identification of key components that need to be considered when designing a secure architecture
    - A practical blueprint showing an organization how to create the right architecture for secure business collaboration in their enterprise.

From Connectivity to Collaboration



Principles - 1

Fundamentals

- The scope and level of protection must be specific and appropriate to the asset at risk
- Security mechanisms must be pervasive, simple, scalable and easy to manage
- Assume context at your peril

Survival in a Hostile World

- Devices and applications must communicate using open, secure protocols.
- All devices must be capable of maintaining their security policy on an untrusted network

Principles - 2

Trust

- All people, processes, technology must have declared and transparent levels of trust for any transaction to take place.
- Mutual trust assurance levels must be determinable.

Identity Management and Federation

- Authentication, authorisation and accountability must interoperate / exchange outside of your locus / area of control

Access to Data

- Access to data should be controlled by security attributes of the data itself.
- Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges.
- By default, data must be appropriately secured both in storage and in transit.